CLAIMS

What is claimed is:

1. A method comprising:

establishing a master secret between a first communications device and a second communications device;

opening a connection between the first communications device and the second communications device;

generating a connection secret from the master secret; and

using the connection secret for symmetric key cryptography during the connection.

2. The method of claim 1, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret; and

sending one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher.

3. The method of claim 1, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret;

receiving one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher; and

decrypting the data using the initialized cipher.

4. The method of claim 1, wherein generating the connection secret comprises generating an initialization vector and determining the connection secret using the master secret and the initialization vector.

5. The method of claim 4, wherein the initialization vector comprises a temporal parameter.

6. The method of claim 5, wherein the temporal parameter comprises an absolute frame number related to the opening of the connection.

7. The method of claim 4, wherein the initialization vector comprises one or more air interface parameters.

8. The method of claim 7, wherein the air interface parameters comprise a slot number and a frequency band identifier of a channel allocated to the connection.

9. The method of claim 4, wherein the first communications device does not sent the initialization vector to the second communications device.

10. The method of claim 1, further comprising:

opening a second connection between the first communications device and the second communications device;

generating a second connection secret from the master secret; and

using the second connection secret for symmetric key cryptography during the second connection.

11. The method of claim 1, wherein the connection comprises a communications stream.

12. The method of claim 2, wherein the cipher comprises a stream cipher.

13. The method of claim 12, wherein the stream cipher comprises an RC4 cipher.

14. A communications device comprising:

a memory to store a master secret being known only by the communications device and a second communications device;

a secret generation module coupled to the memory to generate a connection secret from the master secret in response to the communications device opening a connection with the second communications device; and

an symmetric key cryptography module to use the connection secret during the connection for symmetric key cryptography.

15. The communications device of claim 14, wherein the symmetric key cryptography module uses the connection secret as a symmetric key when encrypting data.

16. The communications device of claim 15, wherein the symmetric key cryptography module initializes a cipher with the connection secret.

17. The communications device of claim 15, further comprising a transmitter to send one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher.

18. The communications device of claim 14, wherein the symmetric key cryptography module uses the connection secret as a symmetric key when decrypting encrypted data.

19. The communications device of claim 18, wherein the symmetric key cryptography module initializes a cipher with the connection secret.

20. The communications device of claim 15, further comprising a receiver to receive one or more bursts over the connection, the one or more bursts carrying the encrypted data.

21. The communications device of claim 14, further comprising an air-interface device coupled to the secret generation module to establish and maintain the connection.

22. The communications device of claim 21, wherein the secret generation module generates the connection secret using a temporal parameter related to the connection.

23. The communications device of claim 22, wherein the temporal parameter comprises an absolute frame number related to the opening of the connection by the air-interface module.

24. The communications device of claim 21, wherein the secret generation module generates the connection secret using one or more air interface parameter related to the connection.

25. The communications device of claim 24, wherein the one or more air interface parameters comprise a slot number and a frequency band identifier of a channel allocated to the connection from the air-interface module.

26. A machine-readable medium storing data representing instructions that, when executed by a processor of a first communications device, cause the processor to perform operations comprising:

establishing a master secret between the first communications device and a second communications device;

opening a connection between the first communications device and the second communications device;

generating a connection secret from the master secret; and

using the connection secret for symmetric key cryptography during the connection.

27. The machine-readable medium of claim 26, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret; and

sending one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher.

28. The machine-readable medium of claim 26, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret;

receiving one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher; and

decrypting the data using the initialized cipher.

29. The machine-readable medium of claim 26, wherein generating the connection secret comprises generating an initialization vector and determining the connection secret using the master secret and the initialization vector.

30. The machine-readable medium of claim 29, wherein the initialization vector comprises a temporal parameter.

31. The machine-readable medium of claim 30, wherein the temporal parameter comprises an absolute frame number related to the opening of the connection.

32. The machine-readable medium of claim 29, wherein the initialization vector comprises one or more air interface parameters.

33. The machine-readable medium of claim 32, wherein the air interface parameters comprise a slot number and a frequency band identifier of a channel allocated to the connection.

34. The machine-readable medium of claim 29, wherein the first communications device does not sent the initialization vector to the second communications device.

35. The machine-readable medium of claim 26, wherein the instructions further cause the processor to perform operations comprising:

opening a second connection between the first communications device and the second communications device;

generating a second connection secret from the master secret; and

using the second connection secret for symmetric key cryptography during the second connection.

36. The machine-readable medium of claim 26, wherein the connection comprises a communications stream.

37. The machine-readable medium of claim 2, wherein the cipher comprises a stream cipher.